TÜV NORD

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-11074-01-00

Certificate

No. SEBS-A.123324/14 V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies to

PROGNOST Systems GmbH

Daimlerstraße 10
48432 Rheine

that the safety related machine protection system

PROGNOST®-SILver, 2nd generation

is capable for safety related applications and meet the requirements listed in the following standards.

- **IEC 61508-1/-2/-3: 2010, capable up to SIL 3**
- **IEC 62061:2005 + A1:2012 + A2:2015+CSV/COR1:2015, capable up to SIL_{CL} 3**

Certification program Leittechnik (SEB-ZE-SEECERT-VA-320-20, Rev. 5.1 / 04.19)

The certification is based on the report No. SEBS-A.123324/14TB in the valid version.
This certificate entitles the holder to use the pictured Safety Approved mark.

Expiry date: 2025-01-24
Reference No.: 8111546455

Hamburg, 2020-01-24

B. Pfuff

Bianca Pfuff

Voluntary Certification
TÜV NORD
TÜV NORD Systems GmbH & Co. KG
Safety Approved
PROGNOST®-SILver,
2nd generation
IEC 61508-1/-2/-3: 2010, SIL 3
IEC 62061:2015, SIL_{CL} 3
SEBS-A.123324/14

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany

4 SIL Classification (Extract from the PROGNOST®-SILver2_User Manual, page 83 - 87)

4.1 Conformity to IEC 61508 (SIL)

4.1.1 General Description

The safety Integrity Level (SIL) is one of four levels classifying the requirements for the integrity of the safety-relevant functions allocated to the E/E/PE (safety system). Safety Integrity Level 4 is the highest level of safety integrity and safety Integrity Level 1 is the lowest.

4.1.2 General Information on Classification

In accordance with danger and risk analyses undertaken, needs have grown for risk reduction, which is identified in safety life cycles as derived from the safety requirements. Several common methods and mechanisms are described in this safety requirements. These requirements have also been subdivided into specific safety functions relevant to defined tasks. In addition to the classification of the common safety requirements as specific safety functions, some measurement of the reliability or integrity of the safety functions is also necessary.

The SIL is a means of evaluating electrical / electronic / programmable electronic (E/E/PE) systems concerning to the reliability of their safety functions.

The measurements have been graded and given the name SIL (Safety Integrity Level). The safety integrity of a system can be more accurately defined as “the probability that a safety-related system performs its necessary safety-relevant function under all given conditions within an established period of time“. The specification covers the safety-related functions and the measures to be taken in response to the existing agreed conditions, including the response time needed.

4.1.3 SIL Architecture

PROGNOST®-SILver contains both microcontroller and digital components. It is therefore classified as Complex System. The architecture assumes a one-channel solution (HFT=0). The frequency of the safety function requirement is classified as “Weak”.

Table for “Type B system = complex system“

SFF	HFT (Hardware Fault Tolerance)		
(Safe Failure Fraction)	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% … < 90%	SIL 1	SIL 2	SIL 3
90% … < 99%	SIL 2	SIL 3	SIL4
≥ 99%	SIL 3	SIL4	SIL4

The table shows how the achievable Safety Integrated Level (SIL) of a type B fully safety-relevant complex system is dependent on “Hardware Fault Tolerance“ (HFT) and “Safe Failure Fraction“ (SFF). Further information is available in Part 2 of IEC 61508.

Safety-integrity-Level (SIL)	Operating type – weak requirement frequency (average probability of failure under demand (PFD_{avg})
4	$^{3}10^{-5}$ to < 10^{-4}
3	$^{3}10^{-4}$ to < 10^{-3}
2	$^{3}10^{-3}$ to < 10^{-2}
1	$^{3}10^{-2}$ to < 10^{-1}

This table shows the link between the average probability of failure on demand (PFD_{avg}) and the corresponding SIL for equipment with low demand ratings. Equipment with low demand rating is defined as “equipment in which the safety function is called upon no more than once or twice per year“. The specification applies to the entire safety loop (sensor, logic circuits, and actuators).

4.2 Evaluation according to IEC 61508/61511

Information:

Each PROGNOST®-SILver is able to monitor up to 32 machines. The protection loop evaluation, however, only involves the components relevant to one individual machine.

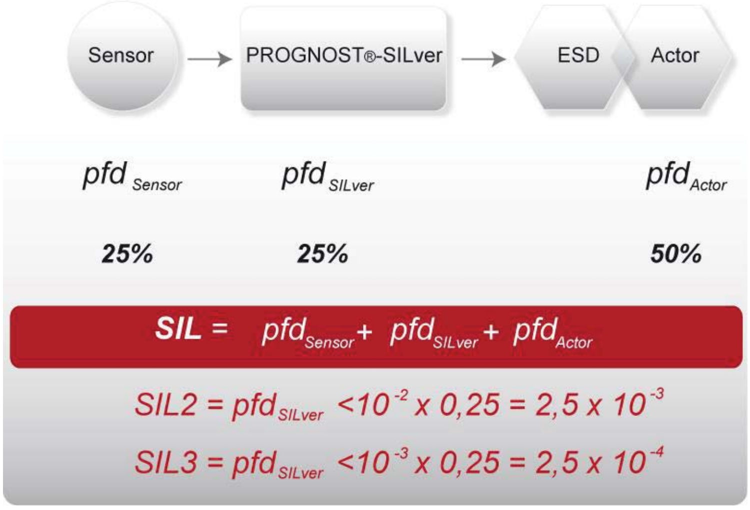
Sensor
PROGNOST®-SILver
ESD
Actor
pfd_{Sensor}
pfd_{SILver}
pfd_{Actor}
25%
25%
50%
$SIL = pfd_{Sensor} + pfd_{SILver} + pfd_{Actor}$
$SIL2 = pfd_{SILver} < 10^{-2} x\ 0,25 = 2,5 x\ 10^{-3}$
$SIL3 = pfd_{SILver} < 10^{-3} x\ 0,25 = 2,5 x\ 10^{-4}$

Figure 4-1 *Safety Instrumented System*

4.2.1 Machine Protection Loop

The figure above shows a possible percentage distribution of the protection loop. The proportions of all included components are summed to give a total value (pfd_{avg}).

$SIL\ 2 = pfd_{avg} = pfd_{Sensor} + pfd_{SILver} + pfd_{Actuator} <= 10^{-2}$

$SIL\ 3 = pfd_{avg} = pfd_{Sensor} + pfd_{SILver} + pfd_{Actuator} <= 10^{-3}$

4.2.1.1 Calculation pfd_{Sensor} (per Machine)

The calculation of the pfd_{sensor} value is based on the safety relevant information from the sensor manufacturer. Some deliver reliability calculation based on a standard with direct pfd_{sensor} output. This is the preferred option. Another option is to use failure rates, that enable you to evaluate the pfd_{sensor} value, for example as follows.

Necessary values:

- λ_{du}= Proportion of dangerous, undetected faults for a sensor (stated in FIT = 1 / 10^{-9} h)
- PTI = Proof Test Interval (stated in h)

This results in the following formula:

$pfd_{Sensor} = \lambda_{du} x\ PTI/2$

Information:

The various values can be obtained from PROGNOST Systems GmbH or the sensor manufacturer.

If the λ_{du} value of a sensor is not available, the MTTF value of the sensor can also be used to calculate the pfd_{Sensor} value of the sensor.

- MTTF = Mean Time To Failure
- $MTTF_d$= Mean Time To Failure dangerous (Interval up to one dangerous fault per sensor)

If MTTF is given, it is usually assumed, that 50 % are dangerous failures, means $MTTF_d$ = 2 x MTTF.

By testing upon failures like open circuit, short circuit, or voltage supply, the signal acquisition cards of PROGNOST®-SILver identify a significant part of all dangerous failures. In the following examples we assume a diagnostic coverage of 95 % of the dangerous failures. Hence the dangerous, undetected failures result in $MTTF_{du} = MTTF_d$ / (1-0,95)

Example:

MTTF = 100.000 hours
$MTTF_d$ = 200.000 hours
$MTTF_{du}$= 4.000.000 hours
PTI= 2 years = 2 x 8.760h = 17.520 h

λ_{du}=1/$MTTF_{du}$ = 1 / 4.000.000 = 2,5x10^{-7} /h = 250 FIT

pfd_{Sensor} = λ_{du}x PTI/2 = 2,5 x 10^{-7} x 17.520 /2 = 2,19 x 10^{-3}

SIL Level: 2,19 x 10^{-3} < 0,25 x 10^{-2} => SIL2 criterion is fulfilled (SIL3 is not)

Information:

For the majority of all sensors, the MTTF value is provided by the manufacturer.

4.2.1.2 Calculation of the pfd_{SILver} (per Channel)

$pfd_{SILver} = pfd_{Signal\_Input} + pfd_{Signal\_Processing} + pfd_{Output}$

Example:

- Signal Input = AI3-B, Eddy Current, PTI = 2 years
- Signal Processing = MP1-2, Machine Protection, PTI = 15 years
- Output = DIO1-2, Relay redundant on one card, PTI = 5 years

pfd_{SILver} = 1,260E-05 +8,933E-05 +2,262E-05 = 12,455E-05 < 2,5 E-04

Conclusion: SIL3 requirement is fulfilled

The different cards of the system offer the following functional safety relevant values:

Table 1: pfd (probability of failure on demand) Values

	PTI	1 year	2 years	3 years	5 years	10 years	15 years	20 years
	Card Type	pfd	pfd	pfd	pfd	pfd	pfd	pfd
Signal Input	AI1-B, ICP	8,074 E-06	1,485 E-05	2,163 E-05	3,519 E-05	6,908 E-05	1,030 E-04	1,369 E-04
	AI2-B, 4..20mA	7,844 E-06	1,442 E-05	2,099 E-05	3,414 E-05	6,700 E-05	9,987 E-05	1,327 E-04
	AI3-B, Eddy Current	7,594 E-06	1,389 E-05	2,020 E-05	3,280 E-05	6,430 E-05	9,580 E-05	1,273 E-04
	AI4-B, Voltage	6,711 E-06	1,231 E-05	1,790 E-05	2,910 E-05	5,708 E-05	8,506 E-05	1,130 E-04
	TI1-B, Trigger	4,125 E-06	7,747 E-06	1,137 E-05	1,861 E-05	3,672 E-05	5,482 E-05	7,293 E-05
	DIO1-2, Input	4,742 E-06	9,484 E-06	1,423 E-05	2,371 E-05	4,742 E-05	7,113 E-05	9,484 E-05
Signal Processing	MP1-2, Machine Protection	n.a.	n.a.	n.a.	n.a.	n.a.	8,933 E-05	1,194 E-04
Output	DIO1-2, Relay (up to SIL2)	5,121 E-06	1,024 E-05	1,536 E-05	2,560 E-05	5,121 E-05	7,681 E-05	1,024 E-04
	DIO1-2, Relay redundant on two cards (up to SIL3)	4,409 E-06	8,819 E-06	1,323 E-05	2,205 E-05	4,410 E-05	6,615 E-05	8,820 E-05
	DIO1-2, Relay redundant on one card (up to SIL3)[1]	4,528 E-06	9,050 E-06	1,357 E-05	2,262 E-05	4,524 E-05	6,786 E-05	9,049 E-05

The values of the table are calculated based on the assumption, that the

[1] These pfd values are valid, if both redundant relays are not part of one relay group (RO1-RO4, RO5-RO8 or RO9-RO10). If both relays are part of one group only SIL2 can be reached.

- Mean Time To Restoration (MTTR) = 8 h
- Proof Test Coverage (PTC) = 100 %

Table 2: SFF and DC Values

Card Type	SFF (Safe Failure Fraction)	DC (Diagnostic Coverage)
AI1-B, ICP	> 99 %	> 90 %
AI2-B, 4..20mA	> 99 %	> 90 %
AI3-B, Eddy Current	> 99 %	> 90 %
AI4-B, Voltage	> 99 %	> 90 %
TI1-B, Trigger	> 99 %	> 90 %
MP1-2, Machine Protection	> 99 %	> 90 %
DIO1-2, Input / Relay	> 99 %	> 90 %